



Avaya Solution & Interoperability Test Lab

Application Notes for dvsAnalytics Encore 6.0.4 with Avaya Proactive Contact 5.1.1 with CTI and Avaya Aura® Application Enablement Services 6.3.3 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for dvsAnalytics Encore 6.0.4 to interoperate with Avaya Proactive Contact 5.1.1 with CTI and Avaya Aura® Application Enablement Services 6.3.3. dvsAnalytics Encore is a call recording solution.

In the compliance testing, dvsAnalytics Encore used the Event Services interface from Avaya Proactive Contact and the Telephony Services Application Programmer Interface from Avaya Aura® Application Enablement Services to obtain information on agent states and calls, and used the Service Observing feature and virtual IP softphones via the Avaya Aura® Application Enablement Services Device, Media, and Call Control interface to capture the media associated with monitored agents for call recording.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration steps required for dvsAnalytics Encore 6.0.4 to interoperate with Avaya Proactive Contact 5.1.1 with CTI and Avaya Aura® Application Enablement Services 6.3.3. dvsAnalytics Encore is a call recording solution.

In the compliance testing, dvsAnalytics Encore used the Event Services interface from Avaya Proactive Contact and the Telephony Services Application Programmer Interface (TSAPI) from Avaya Aura® Application Enablement Services to obtain information on agent states and calls, and used the Service Observing feature and virtual IP softphones via the Avaya Aura® Application Enablement Services Device, Media, and Call Control (DMCC) interface to capture the media associated with monitored agents for call recording.

The Event Services and TSAPI interfaces are used by dvsAnalytics Encore to monitor agent stations and calls, and the DMCC interface is used by dvsAnalytics Encore to register virtual IP softphones to pick up the media for call recording. dvsAnalytics Encore starts the call recording by sending Service Observing button press from a virtual IP softphone via the DMCC interface to observe the active call. The Event Services and/or TSAPI event reports are also used to determine when to stop the call recordings.

This compliance test covered the recording of calls using the Avaya Proactive Contact with CTI deployment option.

2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of the Encore application, the application automatically registers virtual IP softphones to Communication Manager using DMCC, requests monitoring on the skill groups and agent stations using TSAPI, and requests monitoring of agent states and call events using Event Services.

For the manual part of testing, each call was handled manually on the agent station with generation of unique audio content for recordings. Necessary user actions such as hold and reconnect were performed from the agent telephones to test the different call scenarios.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to Encore. The verification of tests included use of Encore logs for proper message exchanges, and use of Encore web interface for proper logging and playback of calls.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on Encore:

- Handling of Event Services agent states and call events.
- Handling of TSAPI messages in the areas of event notification and value queries.
- Use of DMCC registration services to register and un-register virtual IP softphones.
- Use of DMCC physical device services to activate Service Observing for virtual IP softphones to obtain the media.
- Proper recording, logging, and playback of calls for agent blending scenarios involving inbound, outbound, agent drop, customer drop, hold, reconnect, simultaneous calls, conference, and transfer.

The serviceability testing focused on verifying the ability of Encore to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to Encore.

2.2. Test Results

All test cases were executed and verified. The following were observations on Encore from the compliance testing.

- The recording entries for outbound calls delivered by Proactive Contact were reported with Incoming as Call Direction.
- Agent short connections to phantom CTI stations and announcements were included as separate recording entries.
- The held scenario for a Proactive Contact outbound call produced one recording entry, and the held scenario for an inbound ACD call produced one recording entry as well.
- The number of softphones to configure need to take into account the small interval of 500ms that a softphone will not be available between recordings.

2.3. Support

Technical support on Encore can be obtained through the following:

- **Phone:** (800) 910-4564
- **Email:** Support@dvsAnalytics.com

3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**.

The detailed administration of basic connectivity between Communication Manager and Proactive Contact, between Communication Manager and Application Enablement Services, and of contact center devices are not the focus of these Application Notes and will not be described.

In the compliance testing, Encore monitored the skill group and agent station extensions shown in the table below. Note that the skill groups and agent login IDs were associated with the inbound ACD calls for the agent blending mode.

Contact Center Device Type	Extension
Skill Group	41410, 41412
Agent Station	65001, 65002
Agent Login IDs	41661, 41662

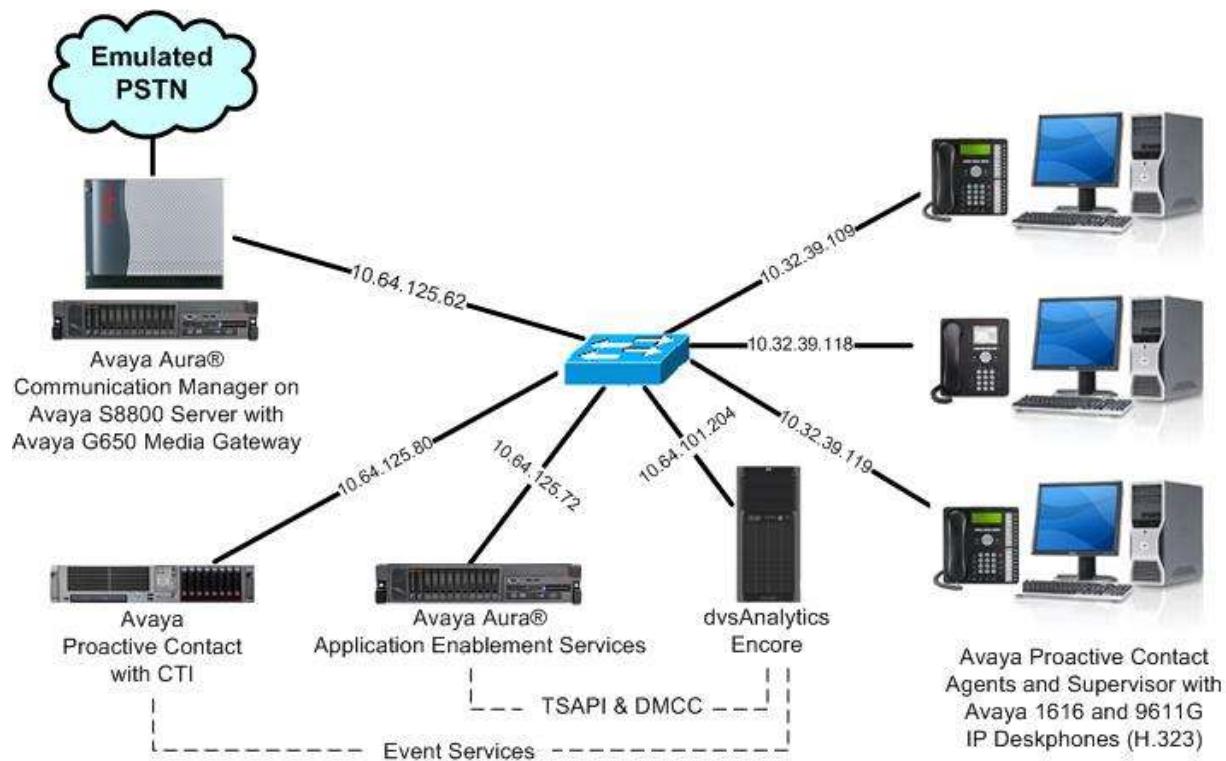


Figure 1: Compliance Testing Configuration

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya Aura® Communication Manager on Avaya S8800 Server with Avaya G650 Media Gateway	6.3.11.1 (R016x.03.0.124.0-22450)
Avaya Aura® Application Enablement Services	6.3.3 SP4 (6.3.3.4.10-0)
Avaya Proactive Contact with CTI	5.1.1
Avaya Proactive Contact Agent	5.1.1
Avaya Proactive Contact Supervisor	5.1.1
Avaya 1616 IP Deskphone (H.323)	1.350B
Avaya 9611G IP Deskphone (H.323)	6.4.0.14
Avaya 9650 IP Deskphone (H.323)	3.230A
dvsAnalytics Encore on Windows Server 2008 R2 Standard <ul style="list-style-type: none">• SP_CMAPI.dll• Avaya TSAPI Windows Client (csta32.dll)• Avaya DMCC XML• Avaya Event Services	6.0.4 SP 1 4.1.8796 6.3.3.103 6.1 5.1.1 Patch 372

5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager. The procedures include the following areas:

- Verify license
- Administer CTI link
- Administer system parameters features
- Administer IP codec set
- Administer class of restriction
- Administer virtual IP softphones
- Administer agent stations

5.1. Verify License

Log into the System Access Terminal (SAT) to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the “display system-parameters customer-options” command to verify that the **Computer Telephony Adjunct Links** customer option is set to “y” on **Page 3**. If this option is not set to “y”, then contact the Avaya sales team or business partner for a proper license file.

display system-parameters customer-options	Page 3 of 11
OPTIONAL FEATURES	
Abbreviated Dialing Enhanced List? y	Audible Message Waiting? y
Access Security Gateway (ASG)? n	Authorization Codes? y
Analog Trunk Incoming Call ID? y	CAS Branch? n
A/D Grp/Sys List Dialing Start at 01? y	CAS Main? n
Answer Supervision by Call Classifier? y	Change COR by FAC? n
ARS? y	Computer Telephony Adjunct Links? y
ARS/AAR Partitioning? y	Cvg Of Calls Redirected Off-net? y
ARS/AAR Dialing without FAC? y	DCS (Basic)? y
ASAI Link Core Capabilities? n	DCS Call Coverage? y
ASAI Link Plus Capabilities? n	DCS with Rerouting? y
Async. Transfer Mode (ATM) PNC? n	

Navigate to **Page 6**, and verify that **Service Observing (Basic)** is set to “y”.

display system-parameters customer-options	Page 6 of 11
CALL CENTER OPTIONAL FEATURES	
Call Center Release: 6.0	
ACD? y	Reason Codes? y
BCMS (Basic)? y	Service Level Maximizer? n
BCMS/VuStats Service Level? y	Service Observing (Basic)? y
BSR Local Treatment for IP & ISDN? y	Service Observing (Remote/By FAC)? y
Business Advocate? n	Service Observing (VDNs)? y
Call Work Codes? y	Timed ACW? y
DTMF Feedback Signals For VRU? y	Vectoring (Basic)? y
Dynamic Advocate? n	Vectoring (Prompting)? y

5.2. Administer CTI Link

Add a CTI link using the “add cti-link n” command, where “n” is an available CTI link number. Enter an available extension number in the **Extension** field. Note that the CTI link number and extension number may vary. Enter “ADJ-IP” in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.

add cti-link 2	Page 1 of 3
CTI LINK	
CTI Link: 2	
Extension: 60100	
Type: ADJ-IP	
Name: AES CTI Link	COR: 1

5.3. Administer System Parameters Features

Use the “change system-parameters features” command to enable **Allow Two Observers in Same Call**, which is located on **Page 11**. Set **Service Observing: Warning Tone** as desired.

change system-parameters features	Page 11 of 20
FEATURE-RELATED SYSTEM PARAMETERS	
CALL CENTER SYSTEM PARAMETERS	
EAS	
Expert Agent Selection (EAS) Enabled? y	
Minimum Agent-LoginID Password Length:	
Direct Agent Announcement Extension:	Delay:
Message Waiting Lamp Indicates Status For: station	
VECTORIZING	
Converse First Data Delay: 0	Second Data Delay: 2
Converse Signaling Tone (msec): 100	Pause (msec): 70
Prompting Timeout (secs): 10	
Interflow-qpos EWT Threshold: 2	
Reverse Star/Pound Digit For Collect Step? n	
Available Agent Adjustments for BSR? n	
BSR Tie Strategy: 1st-found	
Store VDN Name in Station's Local Call Log? n	
SERVICE OBSERVING	
Service Observing: Warning Tone? n	or Conference Tone? n
Service Observing Allowed with Exclusion? n	
Allow Two Observers in Same Call? y	

5.4. Administer IP Codec Set

Use the “change ip-codec-set n” command, where “n” is an existing codec set number used for integration with Encore. For **Audio Codec**, enter “G.711MU”, which is the only codec type supported by Encore.

In the compliance testing, this IP codec set was associated with the IP network region used by the agent stations and virtual IP softphones.

change ip-codec-set 1

Page 1 of 2

IP Codec Set

Codec Set: 1

Audio	Silence	Frames	Packet
Codec	Suppression	Per Pkt	Size (ms)
1: G.711MU	n	2	20
2:			

5.5. Administer Class of Restriction

Enter the “change cor n” command, where “n” is the class of restriction (COR) number used for integration with Encore. Set **Can Be Service Observed** and **Can Be A Service Observer** to “y”, as shown below.

In the compliance testing, this COR was assigned to the agent stations and virtual IP softphones.

change cor 7		Page 1 of 23	
CLASS OF RESTRICTION			
COR Number: 7			
COR Description:			
FRL: 0		APLT? y	
Can Be Service Observed? y		Calling Party Restriction: none	
Can Be A Service Observer? y		Called Party Restriction: none	
Time of Day Chart: 1		Forced Entry of Account Codes? n	
Priority Queuing? n		Direct Agent Calling? n	
Restriction Override: none		Facility Access Trunk Test? n	
Restricted Call List? n		Can Change Coverage? n	

5.6. Administer Virtual IP Softphones

Add a virtual softphone using the “add station n” command, where “n” is an available extension number. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Type:** “4610”
- **Name:** A descriptive name.
- **Security Code:** A desired value.
- **COR:** The class of restriction number from **Section 5.5**.
- **IP SoftPhone:** “y”

add station 65991		Page 1 of 5
STATION		
Extension: 65991	Lock Messages? n	BCC: 0
Type: 4610	Security Code: 65991	TN: 1
Port: IP	Coverage Path 1:	COR: 7
Name: Encore Virtual #1	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
	Time of Day Lock Table:	
Loss Group: 19	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 65991	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english		
Survivable GK Node Name:		
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? y	
	IP Video Softphone? n	

Navigate to **Page 4**, and add a “serv-obsrv” button as shown below.

add station 65991		Page 4 of 6
STATION		
SITE DATA		
Room:		Headset? n
Jack:		Speaker? n
Cable:		Mounting: d
Floor:		Cord Length: 0
Building:		Set Color:
ABBREVIATED DIALING		
List1:	List2:	List3:
BUTTON ASSIGNMENTS		
1: call-appr	7:	
2: call-appr	8:	
3: call-appr	9:	
4: serv-obsrv	10:	
5:	11:	

Repeat this section to administer the desired number of virtual IP softphones. In the compliance testing, four virtual IP softphones were administered, as shown below.

```
list station 65991 count 4
```

STATIONS									
Ext/ Hunt-to	Port/ Type	Name/ Surv GK NN	Move	Room/ Data Ext	Cv1/ Cv2	COR/ COS	Cable/ Jack		
65991	S00090 4610	Encore Virtual #1	no			7 1			
65992	S00093 4610	Encore Virtual #2	no			7 1			
65993	S00096 4610	Encore Virtual #3	no			7 1			
65994	S00099 4610	Encore Virtual #4	no			7 1			

5.7. Administer Agent Stations

Use the “change station n” command, where “n” is the first agent station extension from **Section 3**. For **COR**, enter the class of restriction number from **Section 5.5**.

```
change station 65001
```

STATION									
Extension: 65001	Type: 1616	Port: S00010	Name: CMW Station 1	Lock Messages? n	Security Code: *	Coverage Path 1:	Coverage Path 2:	Hunt-to Station:	BCC: 0 TN: 1 COR: 7 COS: 1 Tests? y
STATION OPTIONS									
Loss Group: 19	Speakerphone: 2-way	Display Language: english	Time of Day Lock Table:	Personalized Ringing Pattern: 1	Message Lamp Ext: 65001	Mute Button Enabled? y	Button Modules: 0		

Repeat this section to administer all stations to be monitored. In the compliance testing, two stations were administered as shown below.

```
list station 65001 count 2
```

STATIONS									
Ext/ Hunt-to	Port/ Type	Name/ Surv GK NN	Move	Room/ Data Ext	Cv1/ Cv2	COR/ COS	Cable/ Jack		
65001	S00010 1616	CMW Station 1	no		1	7 1			
65002	S00049 9611	CMW Station 2	no		1	7 1			

6. Configure Avaya Aura® Application Enablement Services

This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer H.323 gatekeeper
- Restart service
- Obtain Tlink name
- Administer Encore user
- Administer ports
- Verify security database

6.1. Launch OAM Interface

Access the OAM web-based interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of the Application Enablement Services server.

The **Please login here** screen is displayed. Log in using the appropriate credentials.



The screenshot shows the Avaya Application Enablement Services Management Console login interface. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" and "Management Console" is displayed. A red horizontal bar spans the width of the page, with a "Help" link on the right. Below this bar is a central login box with the text "Please login here:" followed by a "Username" label and a text input field. A "Continue" button is positioned below the input field. At the bottom of the page, a red horizontal bar is present, and below it, the copyright notice "Copyright © 2009-2014 Avaya Inc. All Rights Reserved." is displayed.

The **Welcome to OAM** screen is displayed next.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for the user. The left sidebar contains a navigation menu with options: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area shows the "Welcome to OAM" screen, which provides an overview of the OAM web interface and lists the administrative domains it manages: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. A note at the bottom states that these domains can be served by one administrator for all domains or a separate administrator for each domain.

AVAYA Application Enablement Services Management Console

Welcome: User
Last login: Wed Sep 9 07:05:31 2015 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.4.10-0
Server Date and Time: Wed Sep 09 07:21:29 MDT 2015
HA Status: Not Configured

Home | Help | Logout

Home

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
Security
Status
User Management
Utilities
Help

Welcome to OAM

The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- High Availability - Use High Availability to manage AE Services HA.
- Licensing - Use Licensing to manage the license server.
- Maintenance - Use Maintenance to manage the routine maintenance tasks.
- Networking - Use Networking to manage the network interfaces and ports.
- Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.
- Status - Use Status to obtain server status informations.
- User Management - Use User Management to manage AE Services users and AE Services user-related resources.
- Utilities - Use Utilities to carry out basic connectivity tests.
- Help - Use Help to obtain a few tips for using the OAM Help system

Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain.

6.2. Verify License

Select **Licensing** → **WebLM Server Access** in the left pane, to display the **Web License Manager** pop-up screen (not shown), and log in using the appropriate credentials.

The screenshot displays the Avaya Application Enablement Services Management Console with the "Licensing" section selected in the left sidebar. The main content area shows the "Licensing" screen, which provides instructions on how to set up and maintain the WebLM, import licenses, and administer reserved licenses. The left sidebar shows the navigation menu with "Licensing" selected, and sub-options: WebLM Server Address, WebLM Server Access, and Reserved Licenses. The main content area lists the steps for setting up and maintaining the WebLM, importing licenses, and administering reserved licenses.

AVAYA Application Enablement Services Management Console

Welcome: User
Last login: Wed Sep 9 07:05:31 2015 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.4.10-0
Server Date and Time: Wed Sep 09 07:21:29 MDT 2015
HA Status: Not Configured

Home | Help | Logout

Licensing

AE Services
Communication Manager Interface
High Availability
Licensing
WebLM Server Address
WebLM Server Access
Reserved Licenses
Maintenance
Networking

Licensing

If you are setting up and maintaining the WebLM, you need to use the following:

- WebLM Server Address

If you are importing, setting up and maintaining the license, you need to use the following:


- WebLM Server Access

If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:

- Reserved Licenses

The **Web License Manager** screen is displayed. Select **Licensed products** → **APPL_ENAB** → **Application_Enablement** in the left pane, to display the **Application Enablement (CTI)** screen in the right pane.

Verify that there are sufficient licenses for **TSAPI Simultaneous Users** and **Device Media and Call Control**, as shown below.


Web License Manager (WebLM v6.3)
Help About Change Password

WebLM Home
Install license
Licensed products
APPL_ENAB
▼ Application_Enablement
View license capacity
View peak usage
Uninstall license
Server properties
Manage users
Shortcuts
Help for Installed Product

Application Enablement (CTI) - Release: 6 - SID: 10503000
Standard License file

You are here: Licensed Products > Application_Enablement > View License Capacity
License installed on: May 11, 2012 7:07:47 PM -04:00

License File Host IDs: 00-16-3E-48-ED-82

Licensed Features

10 Items Show ALL

Feature (License Keyword)	Expiration date	Licensed capacity
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	16
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	10000
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	16
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	16
Product Notes VALUE_NOTES	permanent	SmallServerTypes: e8300c;e8300d;icc;premio;tn8400;laptop;CtiS MediumServerTypes: ibmx306;ibmx306m;del1950;xen;hs20;hs20_... LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;u... TrustedApplications: IPS_001, BasicUnrestricted; DMCUnrestricted; IXP_001, BasicUnrestricted; DMCUnrestricted; IXN_001, BasicUnrestricted; DMCUnrestricted; PC_001, BasicUnrestricted; DMCUnrestricted; CIE_001, BasicUnrestricted; DMCUnrestricted; OSPC_001, BasicUnrestricted; DMCUnrestricted; VP_001, BasicUnrestricted; DMCUnrestricted; SARETIME_001; VALUE_AES_UNIFIED_CC_DESKTOP_n; CCE_... AdvancedUnrestricted, DMCUnrestricted; CSI; AdvancedUnrestricted, DMCUnrestricted; CSI; AdvancedUnrestricted, DMCUnrestricted; AVA; BasicUnrestricted, AdvancedUnrestricted; DM; CCT_ELITE_CALL_CTRL_001, BasicUnrestricted; DMCUnrestricted, AgentEvents;
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	16
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	10000
DLG VALUE_AES_DLG	permanent	16
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	10000
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	16

6.3. Administer TSAPI Link

Select **AE Services** → **TSAPI** → **TSAPI Links** from the left pane of the **Management Console**, to administer a TSAPI link. The **TSAPI Links** screen is displayed, as shown below. Click **Add Link**.

The screenshot shows the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for the user. The left navigation pane shows "AE Services" expanded, with "TSAPI" selected, and "TSAPI Links" highlighted. The main content area displays the "TSAPI Links" screen, which includes a table with columns: Link, Switch Connection, Switch CTI Link #, ASAI Link Version, and Security. Below the table are buttons for "Add Link", "Edit Link", and "Delete Link".

The **Add TSAPI Links** screen is displayed next.

The **Link** field is only local to the Application Enablement Services server, and may be set to any available number. For **Switch Connection**, select the relevant switch connection from the drop-down list. In this case, the existing switch connection "S8800" is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Retain the default values in the remaining fields.

The screenshot shows the "Add TSAPI Links" screen in the Avaya Application Enablement Services Management Console. The left navigation pane is the same as the previous screenshot, but "Communication Manager Interface" is also visible. The main content area displays the "Add TSAPI Links" form, which includes fields for Link (1), Switch Connection (S8800), Switch CTI Link Number (2), ASAI Link Version (7), and Security (Unencrypted). Below the fields are buttons for "Apply Changes" and "Cancel Changes".

6.4. Administer H.323 Gatekeeper

Select **Communication Manager Interface** → **Switch Connections** from the left pane. The **Switch Connections** screen shows a listing of the existing switch connections.

Locate the connection name associated with the relevant Communication Manager, in this case “S8800”, and select the corresponding radio button. Click **Edit H.323 Gatekeeper**.

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane is expanded to 'Communication Manager Interface' and 'Switch Connections'. The main content area displays a table of switch connections. The table has four columns: Connection Name, Processor Ethernet, Msg Period, and Number of Active Connections. There is one entry with Connection Name 'S8800', Processor Ethernet 'No', Msg Period '30', and Number of Active Connections '1'. Below the table are buttons for 'Edit Connection', 'Edit PE/CLAN IPs', 'Edit H.323 Gatekeeper', 'Delete Connection', and 'Survivability Hierarchy'. The 'Edit H.323 Gatekeeper' button is highlighted.

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
S8800	No	30	1

The **Edit H.323 Gatekeeper** screen is displayed. Enter the IP address of a C-LAN circuit pack or the Processor C-LAN on Communication Manager to be used as H.323 gatekeeper, in this case “10.64.125.32” as shown below. Click **Add Name or IP**.

The screenshot shows the 'Edit H.323 Gatekeeper - S8800' screen. The left navigation pane is the same as the previous screenshot. The main content area has a text input field containing '10.64.125.32' and an 'Add Name or IP' button. Below the input field is the label 'Name or IP Address' and two buttons: 'Delete IP' and 'Back'.

6.5. Restart Service

Select **Maintenance** → **Service Controller** from the left pane, to display the **Service Controller** screen in the right pane. Check **DMCC Service** and **TSAPI Service** as shown below, and click **Restart Service**.

**Application Enablement Services**
Management Console

Welcome: User
Last login: Wed Sep 9 07:05:31 2015 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.4.10-0
Server Date and Time: Wed Sep 09 07:21:29 MDT 2015
HA Status: Not Configured

Maintenance | Service ControllerHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▼ Maintenance

Date Time/NTP Server

▶ Security Database

Service Controller

▶ Server Data

▶ Networking

▶ Security

▶ Status

▶ User Management

Service Controller

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input checked="" type="checkbox"/> DMCC Service	Running
<input type="checkbox"/> CVLAN Service	Running
<input type="checkbox"/> DLG Service	Running
<input type="checkbox"/> Transport Layer Service	Running
<input checked="" type="checkbox"/> TSAPI Service	Running

For status on actual services, please use [Status and Control](#)

StartStopRestart ServiceRestart AE ServerRestart LinuxRestart Web Server

6.6. Obtain Tlink Name

Select **Security** → **Security Database** → **Tlinks** from the left pane. The **Tlinks** screen shows a listing of the Tlink names. A new Tlink name is automatically generated for the TSAPI service. Locate the Tlink name associated with the relevant switch connection, which would use the name of the switch connection as part of the Tlink name. Make a note of the associated Tlink name, to be used later for configuring Encore.

In this case, the associated Tlink name is “AVAYA#S8800#CSTA#AES_125_72”. Note the use of the switch connection “S8800” from **Section 6.3** as part of the Tlink name.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for the user. The main navigation pane on the left lists various services, with "Security" expanded to show "Security Database" and "Tlinks" selected. The main content area shows a single Tlink entry with the name "AVAYA#S8800#CSTA#AES_125_72" and a "Delete Tlink" button.

AVAYA Application Enablement Services Management Console

Welcome: User
Last login: Wed Sep 9 07:05:31 2015 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.4.10-0
Server Date and Time: Wed Sep 09 07:21:29 MDT 2015
HA Status: Not Configured

Security | Security Database | Tlinks Home | Help | Logout


Tlinks

Tlink Name
AVAYA#S8800#CSTA#AES_125_72
Delete Tlink

6.7. Administer Encore User

Select **User Management** → **User Admin** → **Add User** from the left pane, to display the **Add User** screen in the right pane.

Enter desired values for **User Id**, **Common Name**, **Surname**, **User Password**, and **Confirm Password**. For **CT User**, select “Yes” from the drop-down list. Retain the default value in the remaining fields. Click **Apply** at the bottom of the screen (not shown below).



Application Enablement Services
Management Console

Welcome: User
Last login: Wed Sep 9 07:05:31 2015 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.4.10-0
Server Date and Time: Wed Sep 09 07:21:29 MDT 2015
HA Status: Not Configured

User Management | User Admin | Add User

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▼ User Management

▶ Service Admin

▼ User Admin

▪ Add User

▪ Change User Password

▪ List All Users

▪ Modify Default Users

▪ Search Users

▶ Utilities

▶ Help

Add User

Fields marked with * can not be empty.

* User Id

encore

* Common Name

encore

* Surname

encore

* User Password

••••••••

* Confirm Password

••••••••

Admin Note

Avaya Role

None

Business Category

Car License

CM Home

Css Home

CT User

Yes

Department Number

Display Name

Employee Number

Employee Type

Enterprise Handle

Given Name

6.8. Administer Ports

Select **Networking** → **Ports** from the left pane, to display the **Ports** screen in the right pane.

In the **DMCC Server Ports** section, select the radio button for **Unencrypted Port** under the **Enabled** column, as shown below. Retain the default values in the remaining fields.

AVAYA

Application Enablement Services
Management Console

Welcome: User
Last login: Wed Sep 9 07:05:31 2015 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.4.10-0
Server Date and Time: Wed Sep 09 07:21:29 MDT 2015
HA Status: Not Configured

Networking | Ports

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▼ Networking

▶ AE Service IP (Local IP)

▶ Network Configure

▶ Ports

▶ TCP Settings

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Ports

CVLAN Ports

Unencrypted TCP Port 9999

Enabled Disabled

Encrypted TCP Port 9998

DLG Port TCP Port 5678

TSAPI Ports

TSAPI Service Port 450

Enabled Disabled

Local TLINK Ports

TCP Port Min 1024

TCP Port Max 1039

Unencrypted TLINK Ports

TCP Port Min 1050

TCP Port Max 1065

Encrypted TLINK Ports

TCP Port Min 1066

TCP Port Max 1081

DMCC Server Ports

Unencrypted Port 4721

Enabled Disabled

Encrypted Port 4722

TR/87 Port 4723

6.9. Verify Security Database

Select **Security → Security Database → Control** from the left pane, to display the **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** screen in the right pane.

Make certain that **Enable SDB for TSAPI Service, JTAPI and Telephony Web Services** retained the default value of unchecked. In the event that the parameter is enabled with security database used by the customer, then follow reference [2] to configure access privileges for the Encore user from **Section 6.7**.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for the user. The main navigation pane on the left lists various service categories, with "Security" expanded to show "Security Database" and "Control". The right pane shows the "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services" configuration page, which contains two unchecked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services", along with an "Apply Changes" button.

Welcome: User
Last login: Wed Sep 9 07:05:31 2015 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.4.10-0
Server Date and Time: Wed Sep 09 07:21:29 MDT 2015
HA Status: Not Configured

Security | Security Database | Control Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
Security
Account Management
Audit
Certificate Management
Enterprise Directory
Host AA
PAM
Security Database
Control

SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services

☐ Enable SDB for DMCC Service
☐ Enable SDB for TSAPI Service, JTAPI and Telephony Web Services
Apply Changes

7. Configure Avaya Proactive Contact

This section provides the procedures for obtaining information from Proactive Contact. The procedures include the following areas:

- Obtain host name
- Obtain agent IDs

7.1. Obtain Host Name

Log in to the Linux shell of the Proactive Contact server. Use the “`uname -a`” command to obtain the host name, which will be used later for configuring Encore.

In the compliance testing, the host name of the Proactive Contact server is “`lzpds4b`”, as shown below.

```
$ uname -a
Linux lzpds4 2.6.18-371.1.2.el5PAE #1 SMP Mon Oct 7 16:41:57 EDT 2013 i686 i686 i386
GNU/Linux
LZPDS4(XXXXXX)@/opt/avaya/pds [999]
$
```

7.2. Obtain Agent IDs

Navigate to the `/etc` directory, and display the content of the **passwd** file. Note the values of the agent IDs, which will be used later for configuring Encore. The first two agent IDs circled below were used in the compliance testing.

```
$cat passwd
.
.
agent1:x:1105:1102:Test agent1:/home/pds_agent:/bin/rbash
agent2:x:1106:1102:Test agent2:/home/pds_agent:/bin/rbash
.
.
```

8. Configure dvsAnalytics Encore

This section provides the procedures for configuring Encore. The procedures include the following areas:

- Administer softphones
- Administer CTISetup
- Launch CT Gateways
- Administer CT Gateways
- Administer users

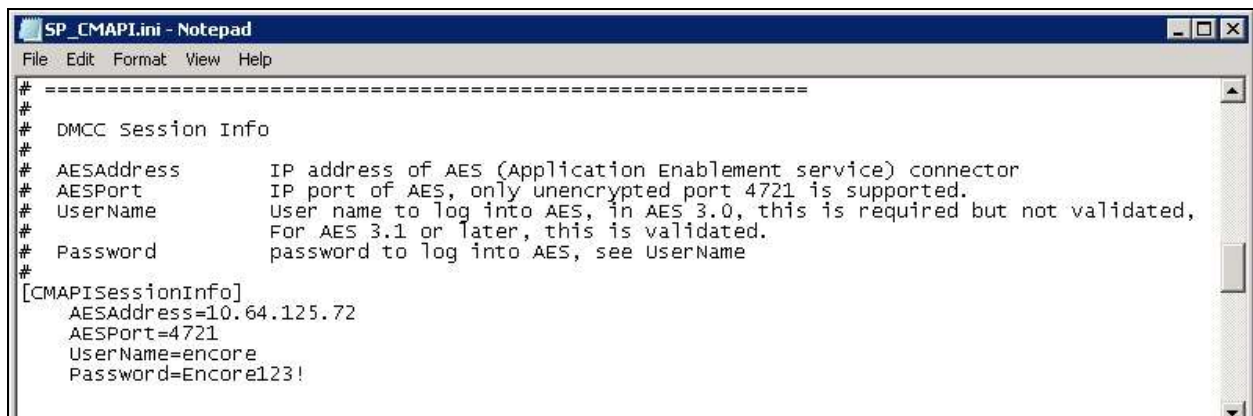
The configuration of Encore is performed by dvsAnalytics installers and dealers. The procedural steps are presented in these Application Notes for informational purposes.

8.1. Administer Softphones

From the Encore server, navigate to the **D:\EncData\Config\Softphone** directory to edit the **SP_CMAPI.ini** file shown below.

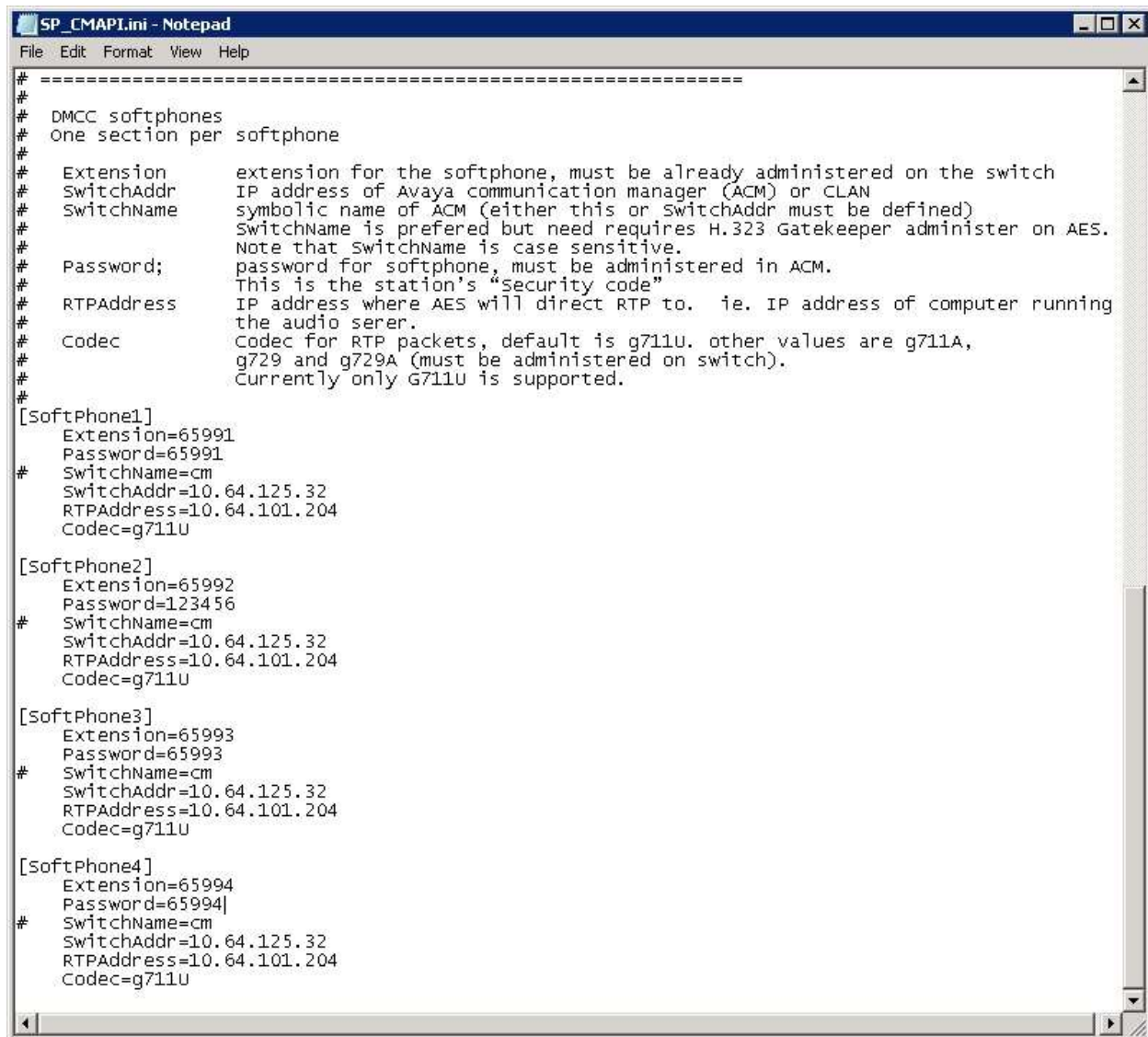


Scroll down to the **DMCC Session Info** sub-section. Under **CMAPISessionInfo**, set **AESAddress** to the IP address of the Application Enablement Services server. Set **UserName** and **Password** to the Encore user credentials from **Section 6.7**. Retain the default value for **AESPort**.



Scroll down to the **DMCC softphones** sub-section. Under **SoftPhone1**, set **Extension** and **Password** to the first virtual IP softphone extension and security code from **Section 5.6**. Set **SwitchAddr** to the IP address of the H.323 Gatekeeper from **Section 6.4**, or set **SwitchName** to the host name of the H.323 Gatekeeper. Set **RTPAddress** to the IP address of the Encore server. Retain the default values in the remaining fields.

Create additional softphone entries as necessary. In the compliance testing, four softphones were configured to correspond to the four virtual IP softphones from **Section 5.6**.



```
# =====
#
# DMCC softphones
# One section per softphone
#
# Extension      extension for the softphone, must be already administered on the switch
# SwitchAddr     IP address of Avaya communication manager (ACM) or CLAN
# SwitchName     symbolic name of ACM (either this or SwitchAddr must be defined)
#                SwitchName is preferred but need requires H.323 Gatekeeper administer on AES.
#                Note that SwitchName is case sensitive.
# Password;      password for softphone, must be administered in ACM.
#                This is the station's "security code"
# RTPAddress     IP address where AES will direct RTP to.  ie. IP address of computer running
#                the audio server.
# Codec          Codec for RTP packets, default is g711u. other values are g711A,
#                g729 and g729A (must be administered on switch).
#                Currently only G711U is supported.
#
[SoftPhone1]
Extension=65991
Password=65991
# SwitchName=cm
SwitchAddr=10.64.125.32
RTPAddress=10.64.101.204
Codec=g711u

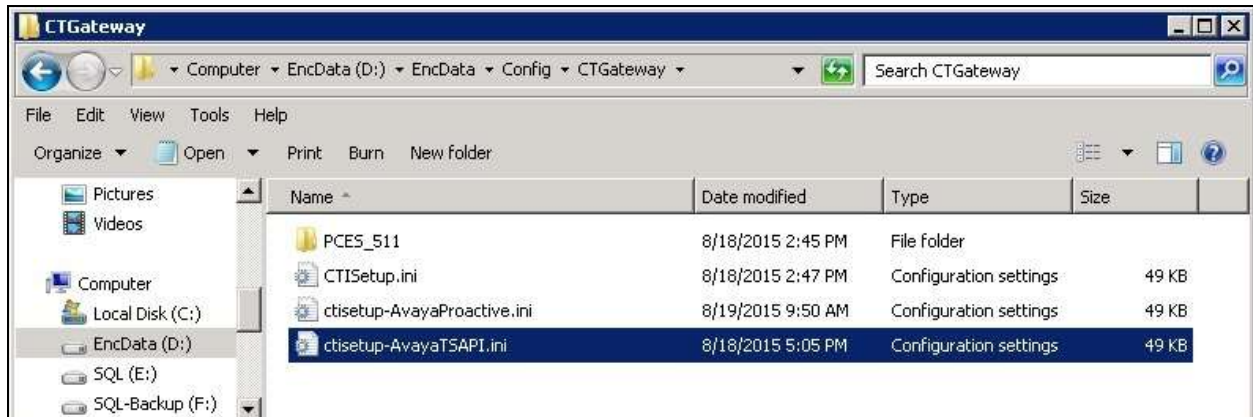
[SoftPhone2]
Extension=65992
Password=123456
# SwitchName=cm
SwitchAddr=10.64.125.32
RTPAddress=10.64.101.204
Codec=g711u

[SoftPhone3]
Extension=65993
Password=65993
# SwitchName=cm
SwitchAddr=10.64.125.32
RTPAddress=10.64.101.204
Codec=g711u

[SoftPhone4]
Extension=65994
Password=65994
# SwitchName=cm
SwitchAddr=10.64.125.32
RTPAddress=10.64.101.204
Codec=g711u
```

8.2. Administer CTISetup

Navigate to the **D:\EncData\Config\CTGateway** directory to edit the applicable **ini** file for TSAPI integration, in this case **ctisetup-AvayaTSAPI.ini**. Note that the file name may vary, and that the file was created by copying from the default **CTISetup.ini** file.

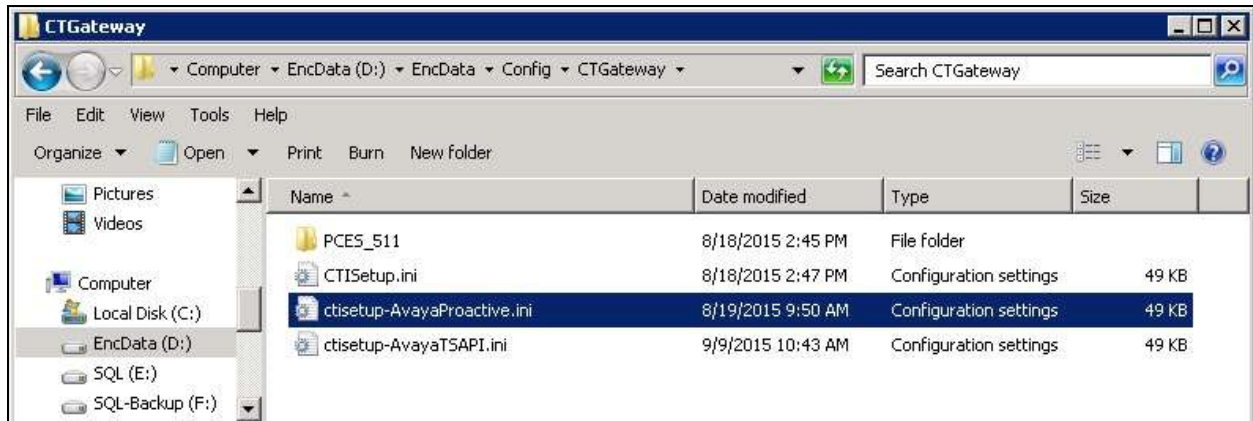


Scroll down to the **ACD paths** sub-section. Under **ACD1**, set **ID** to the first skill group extension from **Section 3**. Create additional ACD entries as necessary when more than one skill group is being monitored.

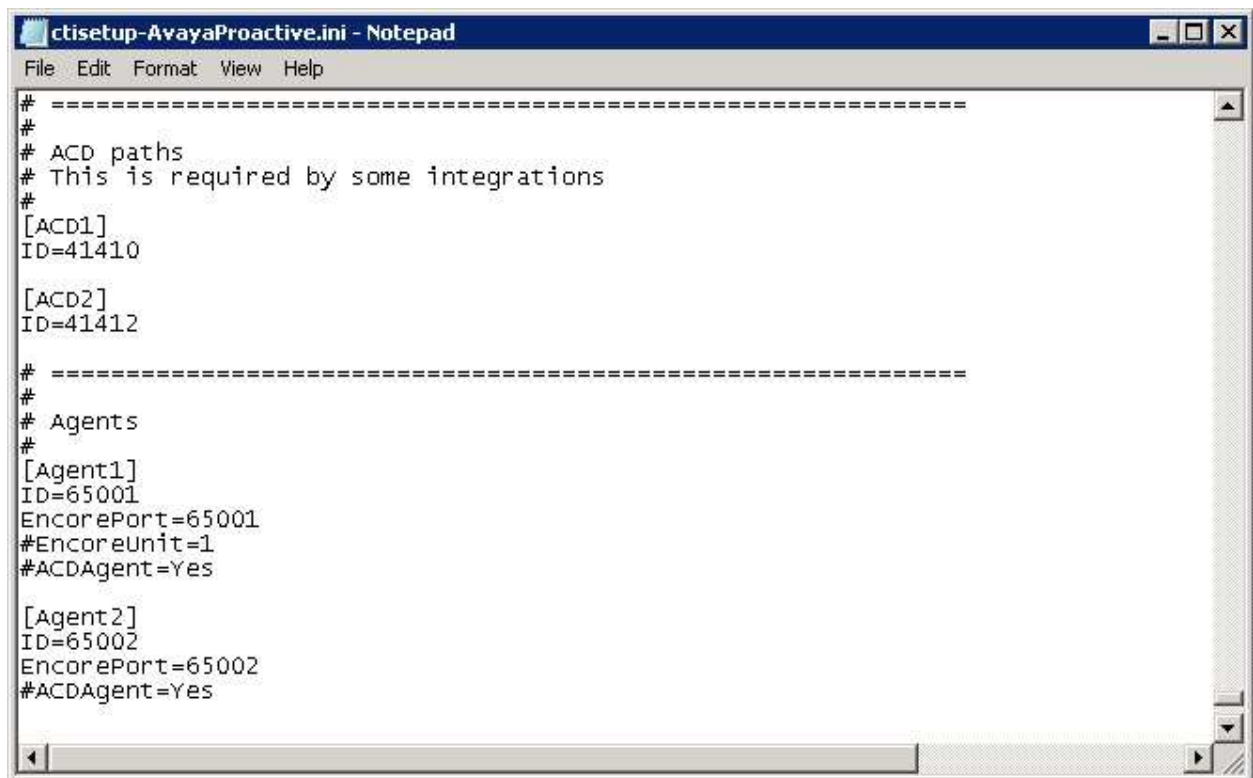
Scroll to the **Agents** sub-section. Under **Agent1**, set **ID** and **EncorePort** to the first agent station extension from **Section 3**. Create additional agent entries as necessary when more than one agent is being monitored.



In the same **D:\EncData\Config\CTGateway** directory, edit the applicable **ini** file for Event Services integration, in this case **ctisetaup-AvayaProactive.ini**. Note that the file name may vary, and that the file was created by copying from the default **CTISetup.ini** file.



Scroll down to the **ACD paths** and **Agents** sub-sections, and make the same changes as described above for **ctisetaup -AvayaTSAPI.ini**.

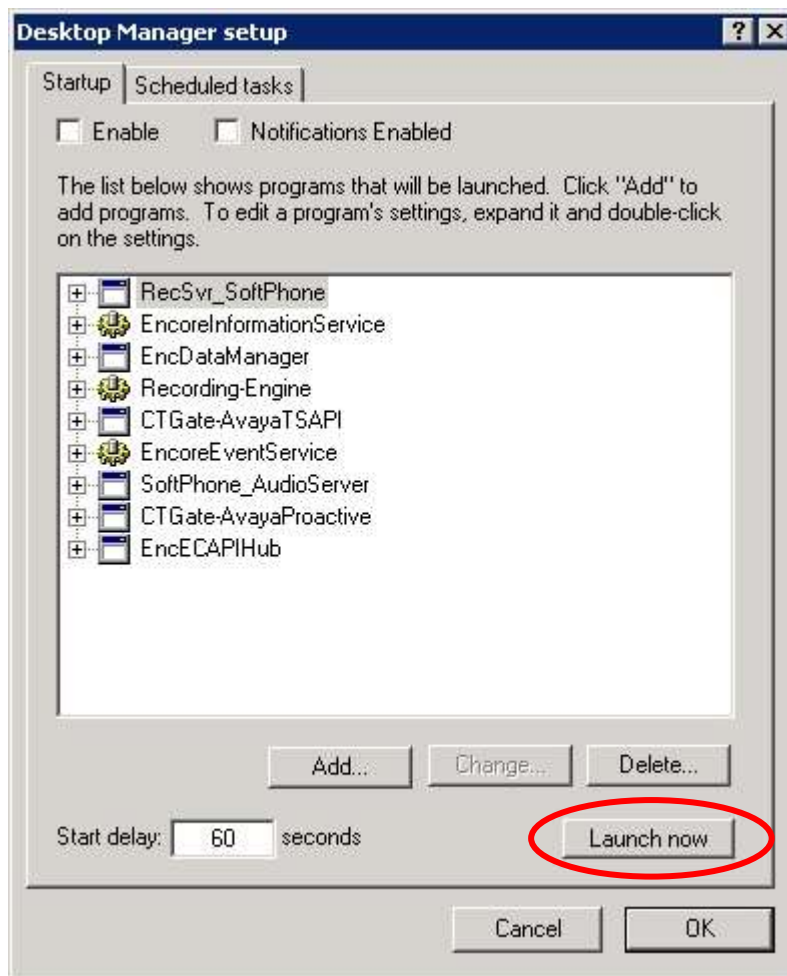


8.3. Launch CT Gateways

Right click on the **Desktop Manager** icon from the system tray shown below, and select **Configure** (not shown).



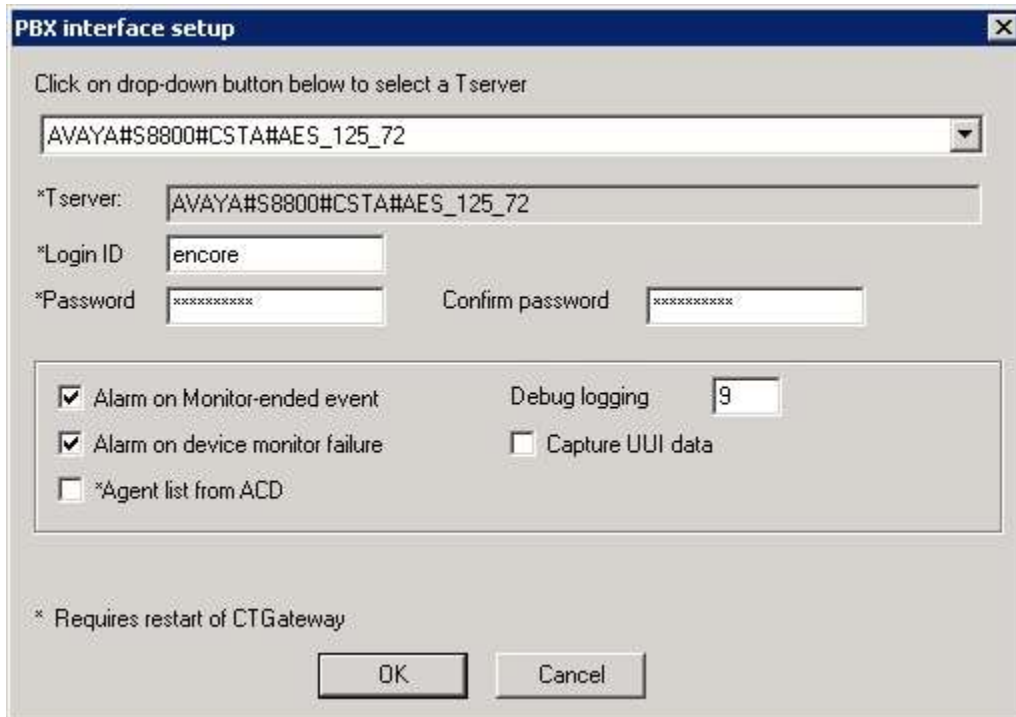
The **Desktop Manager setup** screen is displayed. Click **Launch now** to launch the CT Gateways.



8.4. Administer CT Gateways

The **CT Gateway (AvayaTSAPI)** and **CT Gateway (AvayaProactive)** screens are displayed (not shown). From the **CT Gateway (AvayaTSAPI)** screen, select **PBX → Configure** from the top menu (not shown).

The **PBX interface setup** screen below is displayed. Select the Tlink name in **Section 6.6** from the drop-down list. For **Login ID**, **Password**, and **Confirm password**, enter the Encore user credentials from **Section 6.7**. Retain the default values in the remaining fields.



The image shows a 'PBX interface setup' dialog box. It has a title bar with a close button. Inside, there's a text instruction: 'Click on drop-down button below to select a Tserver'. Below this is a drop-down menu showing 'AVAYA#S8800#CSTA#AES_125_72'. Below the menu are three text input fields: '*Tserver:' (containing 'AVAYA#S8800#CSTA#AES_125_72'), '*Login ID' (containing 'encore'), and '*Password' (containing 'xxxxxxxx'). To the right of the password field is a 'Confirm password' field (containing 'xxxxxxxx'). Below these fields is a group box containing three checkboxes: 'Alarm on Monitor-ended event' (checked), 'Alarm on device monitor failure' (checked), and '*Agent list from ACD' (unchecked). To the right of these checkboxes is a 'Debug logging' field (containing '9') and a 'Capture UUI data' checkbox (unchecked). At the bottom left, there's a note: '* Requires restart of CTGateway'. At the bottom right, there are 'OK' and 'Cancel' buttons.

PBX interface setup

Click on drop-down button below to select a Tserver

AVAYA#S8800#CSTA#AES_125_72

*Tserver: AVAYA#S8800#CSTA#AES_125_72

*Login ID: encore

*Password: xxxxxxxx Confirm password: xxxxxxxx

☒ Alarm on Monitor-ended event ☐ Debug logging 9

☒ Alarm on device monitor failure ☐ Capture UUI data

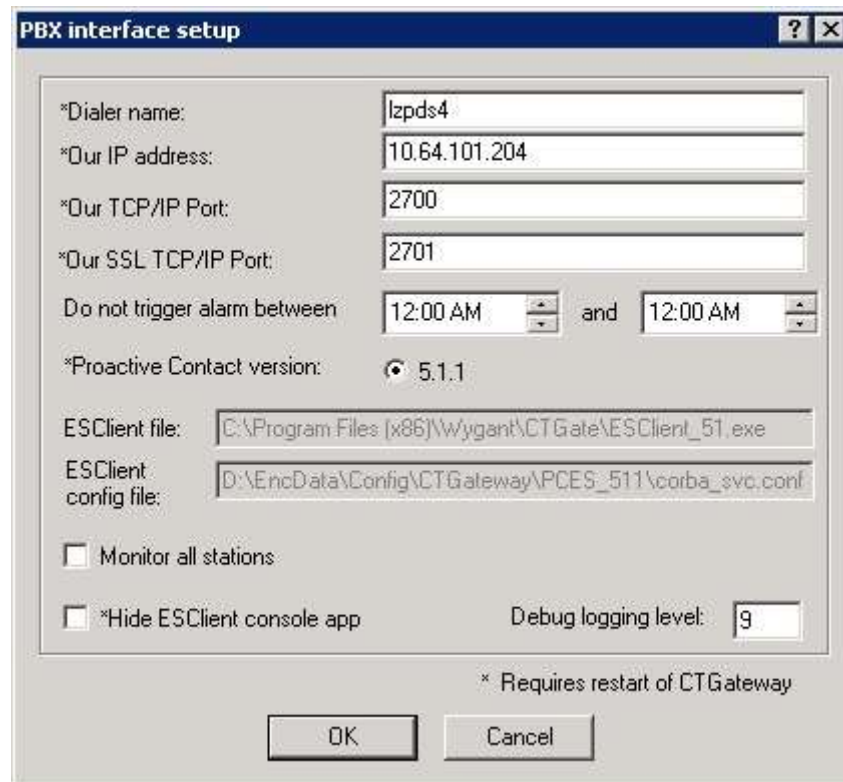
☐ *Agent list from ACD

* Requires restart of CTGateway

OK Cancel

From the **CT Gateway (AvayaProactive)** screen (not shown), select **PBX → Configure** from the top menu (not shown).

The **PBX interface setup** screen below is displayed. For **Dialer name**, enter the host name of Proactive Contact from **Section 7.1**. For **Our IP address**, enter the IP address of the Encore server. Retain the default values in the remaining fields.



The image shows a Windows-style dialog box titled "PBX interface setup". It contains several input fields and checkboxes. The fields are: "*Dialer name:" with the value "lzpds4"; "*Our IP address:" with the value "10.64.101.204"; "*Our TCP/IP Port:" with the value "2700"; "*Our SSL TCP/IP Port:" with the value "2701"; "Do not trigger alarm between:" with two time pickers both set to "12:00 AM" and the word "and" between them; "*Proactive Contact version:" with a radio button selected next to "5.1.1"; "ESClient file:" with the path "C:\Program Files (x86)\Wygant\CTGate\ESClient_51.exe"; and "ESClient config file:" with the path "D:\EncData\Config\CTGateway\PCES_511\corba_svc.conf". There are two checkboxes: "Monitor all stations" (unchecked) and "*Hide ESClient console app" (unchecked). A "Debug logging level:" field has the value "9". At the bottom right, there is a note "* Requires restart of CTGateway". At the bottom center are "OK" and "Cancel" buttons.

*Dialer name:	lzpds4
*Our IP address:	10.64.101.204
*Our TCP/IP Port:	2700
*Our SSL TCP/IP Port:	2701
Do not trigger alarm between	12:00 AM and 12:00 AM
*Proactive Contact version:	<input checked="" type="radio"/> 5.1.1
ESClient file:	C:\Program Files (x86)\Wygant\CTGate\ESClient_51.exe
ESClient config file:	D:\EncData\Config\CTGateway\PCES_511\corba_svc.conf
<input type="checkbox"/> Monitor all stations	
<input type="checkbox"/> *Hide ESClient console app	Debug logging level: 9

* Requires restart of CTGateway

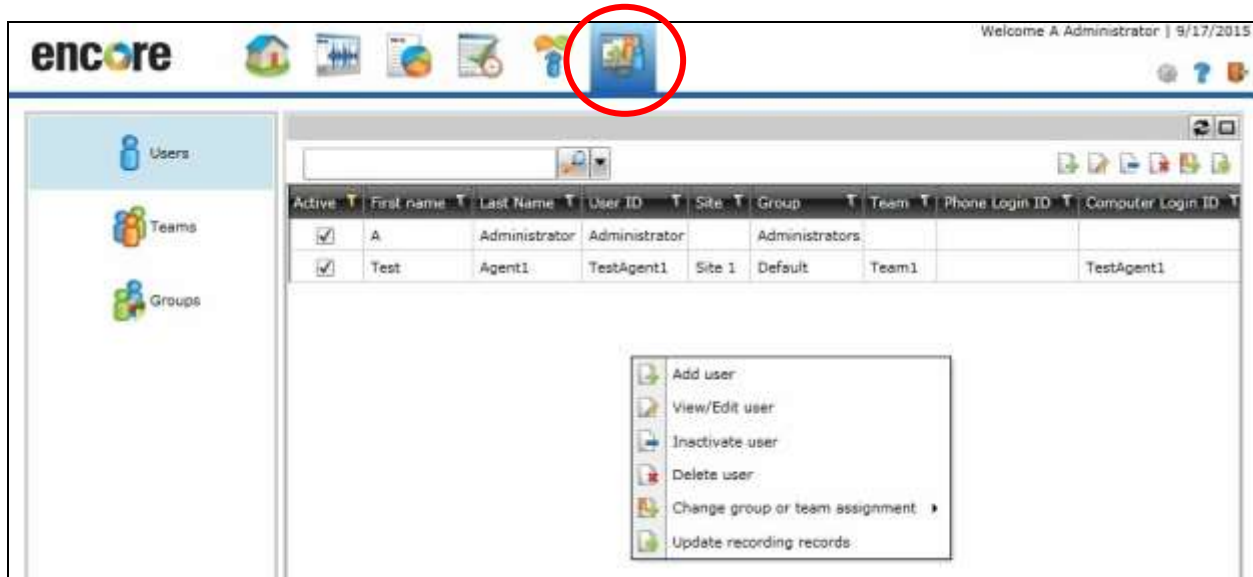
OK Cancel

8.5. Administer Users

Access the Encore web interface by using the URL “http://ip-address/encore” in an Internet browser window, where “ip-address” is the IP address of the Encore server. The **encore** screen is displayed. Click **Login** and log in using the appropriate credentials.

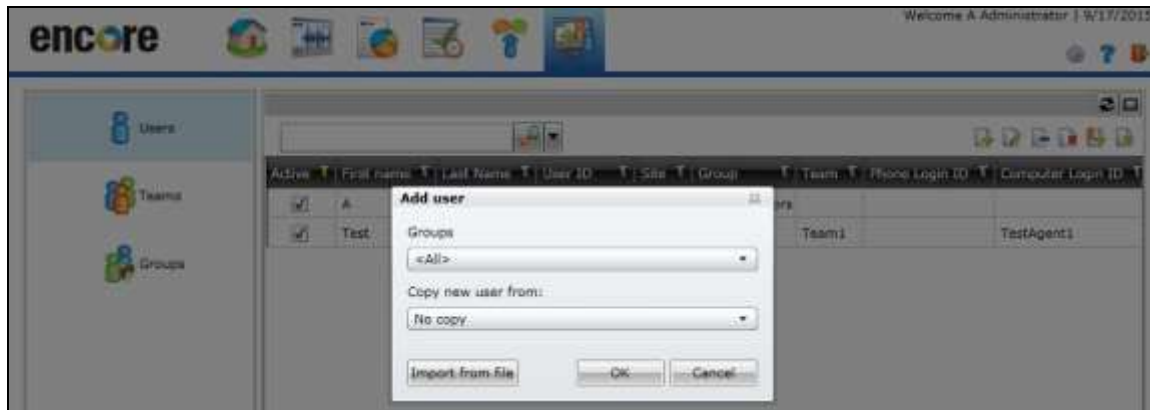


In the updated **encore** screen, click the **User and System Configuration** icon from the top menu, followed by **Users** in the left pane, to display a list of users shown below. Right click in the right pane and select **Add user**.

The image shows the Encore user management interface. At the top, there is a navigation bar with the 'encore' logo and several icons. The 'User and System Configuration' icon is circled in red. Below the navigation bar, there is a left pane with 'Users', 'Teams', and 'Groups' options. The main area displays a table of users. A right-click context menu is open over the table, showing options like 'Add user', 'View/Edit user', 'Inactivate user', 'Delete user', 'Change group or team assignment', and 'Update recording records'.

Active	First name	Last Name	User ID	Site	Group	Team	Phone Login ID	Computer Login ID
<input checked="" type="checkbox"/>	A	Administrator	Administrator		Administrators			
<input checked="" type="checkbox"/>	Test	Agent1	TestAgent1	Site 1	Default	Team1		TestAgent1

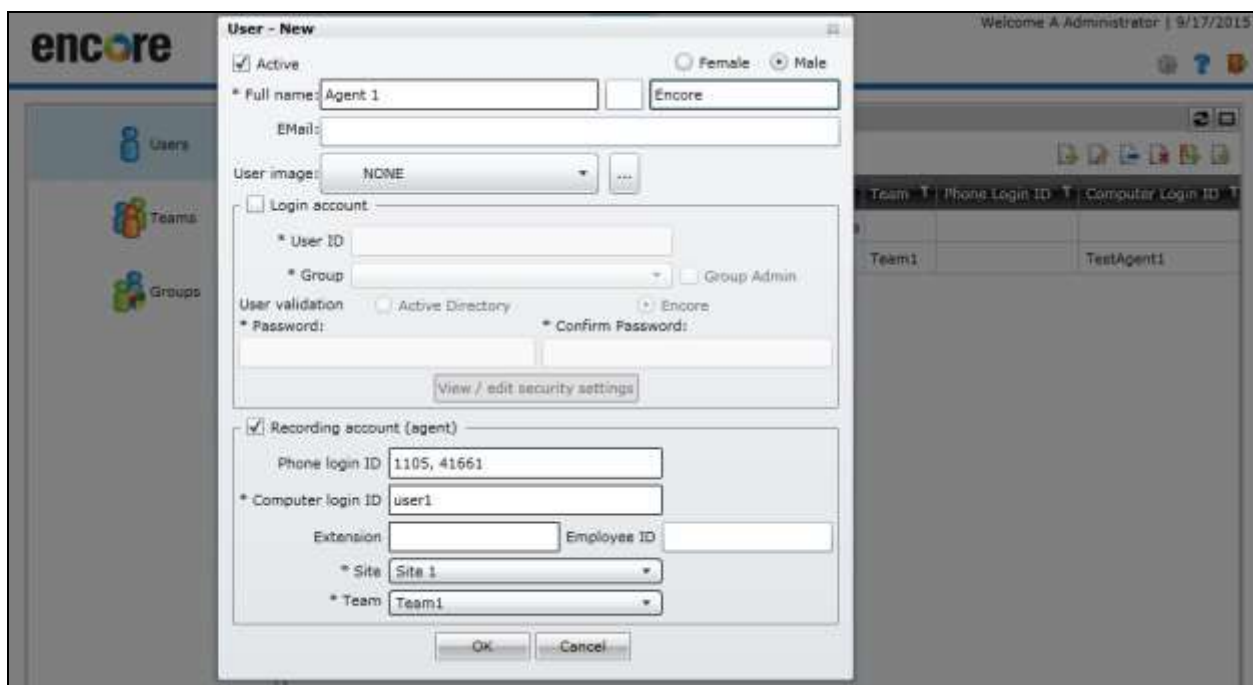
The **Add user** pop-up screen is displayed. Retain all default values and click **OK**.



The **User - New** pop-up screen is displayed next. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Female/Male:** Select the applicable radio button.
- **Full name:** Enter desired name for the agent.
- **Recording account (agent):** Check this field.
- **Computer login ID:** Enter a desired value.
- **Site:** Select the applicable pre-configured site.
- **Team:** Select the applicable pre-configured team.

For **Phone login ID**, enter the applicable Proactive Contact agent ID from **Section 7.2**, and the applicable ACD agent login ID from **Section 3** for the agent, as shown below.



Repeat this section to administer all users that will be recorded. In the compliance testing, two users were created to associate with the two agents from **Section 3**, as shown below.



The screenshot shows the Encore user management interface. On the left is a sidebar with 'Users', 'Teams', and 'Groups' options. The main area displays a table of users. The table has columns for Active status, First name, Last Name, User ID, Site, Group, Team, Phone Login ID, and Computer Login ID. There are four rows of data: an Administrator user, a TestAgent1 user, and two agent users (Agent 1 and Agent 2) associated with Site 1 and Team 1.

Active	First name	Last Name	User ID	Site	Group	Team	Phone Login ID	Computer Login ID
<input checked="" type="checkbox"/>	A	Administrator	Administrator		Administrators			
<input checked="" type="checkbox"/>	Test	Agent1	TestAgent1	Site 1	Default	Team1		TestAgent1
<input checked="" type="checkbox"/>	Agent 1	Encore		Site 1		Team1	1105, 41661	user1
<input checked="" type="checkbox"/>	Agent 2	Encore		Site 1		Team1	1106, 41662	user2

9. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Proactive Contact, Application Enablement Services, and Encore.

9.1. Verify Avaya Aura® Communication Manager

On Communication Manager, verify status of the administered CTI link by using the “status aesvcs cti-link” command. Verify that **Service State** is “established” for the relevant CTI link, as shown below.

```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1		no		down	0	0
2	7	no	aes_125_72	established	62	74

Verify the registration status of virtual IP softphones by using the “list registered-ip-stations” command. Verify that all softphone extensions from **Section 5.6** are displayed, as shown below.

```
list registered-ip-stations
```

REGISTERED IP STATIONS					
Station Ext or Orig Port	Set Type/ Net Rgn	Prod ID/ Release	TCP Skt	Station IP Address/ Gatekeeper IP Address	
65000	9650	IP_Phone	y	10.32.39.119	
	1	3.230A		10.64.125.62	
65001	1616	IP_Phone	y	10.32.39.109	
	1	1.350B		10.64.125.62	
65002	9611	IP_Phone	y	10.32.39.118	
	1	6.4014		10.64.125.62	
65991	4610	IP_API_A	y	10.64.125.72	
	1	3.2040		10.64.125.32	
65992	4610	IP_API_A	y	10.64.125.72	
	1	3.2040		10.64.125.32	
65993	4610	IP_API_A	y	10.64.125.72	
	1	3.2040		10.64.125.32	
65994	4610	IP_API_A	y	10.64.125.72	
	1	3.2040		10.64.125.32	

9.2. Verify Avaya Proactive Contact

Log in to the Linux shell of the Proactive Contact server, and issue the “netstat | grep enservice” command. Verify that there is an entry showing an **ESTABLISHED** connection between Proactive Contact and Encore, as shown below.

tcp	0	0	lzpds4:enservice_ssl	10.64.101.204:60851	ESTABLISHED
tcp	0	0	lzpds4:enservice_ssl	lzpds4:61636	ESTABLISHED
tcp	0	0	lzpds4:61636	lzpds4:enservice_ssl	ESTABLISHED

9.3. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, verify status of the TSAPI link by selecting **Status** → **Status and Control** → **TSAPI Service Summary** from the left pane. The **TSAPI Link Details** screen is displayed.

Verify that **Status** is “Talking” for the relevant TSAPI link, as shown below.

AVAYA

Application Enablement Services
Management Console

Welcome: User
Last login: Fri Sep 18 12:31:35 2015 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.4.10-0
Server Date and Time: Fri Sep 18 12:33:55 MDT 2015
HA Status: Not Configured

Status | Status and Control | TSAPI Service SummaryHome | Help | Logout

AE Services

Communication Manager

Interface

High Availability

Licensing

Maintenance

Networking

Security

Status

Alarm Viewer

Log Manager

Logs

Status and Control

CVLAN Service Summary

DLG Services Summary

DMCC Service Summary

Switch Conn Summary

TSAPI Service Summary

TSAPI Link Details


☐ Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
<input checked="" type="radio"/>	1	S8800	2	Talking	Fri Sep 11 11:39:28 2015	Online	16	10	75	63	30

For service-wide information, choose one of the following:

Verify status of the DMCC link by selecting **Status → Status and Control → DMCC Service Summary** from the left pane. The **DMCC Service Summary – Session Summary** screen is displayed.

In the lower portion of the screen, verify that there is an active session with the Encore user name from **Section 6.7**, and that **# of Associated Devices** reflects the number of softphones from **Section 8.1**.



Application Enablement Services

Management Console

Welcome: User
 Last login: Fri Sep 18 12:31:35 2015 from 10.32.39.20
 Number of prior failed login attempts: 0
 HostName/IP: aes_125_72/10.64.125.72
 Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
 SW Version: 6.3.3.4.10-0
 Server Date and Time: Fri Sep 18 12:33:28 MDT 2015
 HA Status: Not Configured

Status | Status and Control | DMCC Service Summary
Home | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▼ **Status**
 - Alarm Viewer
 - Log Manager
 - ▶ Logs
 - ▼ **Status and Control**
 - CVLAN Service Summary
 - DLG Services Summary
 - **DMCC Service Summary**
 - Switch Conn Summary
 - TSAPI Service Summary

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)
Generated on Fri Sep 18 12:33:28 MDT 2015

Service Uptime: 2 days, 5 hours 9 minutes

Number of Active Sessions: 1

Number of Sessions Created Since Service Boot: 7

Number of Existing Devices: 4

Number of Devices Created Since Service Boot: 49

	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	8EFF0798AB72FC2F9 B4CD613EEFAED9D-6	encore	SPAS1	10.64.101.204	XML Unencrypted	4

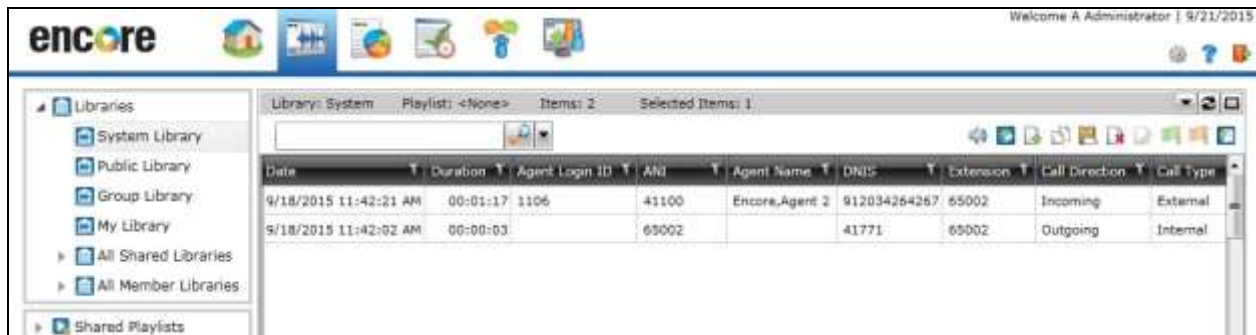
Terminate Sessions
Show Terminated Sessions

Item 1-1 of 1
1 Go

9.4. Verify dvsAnalytics Encore

Start a job on Proactive Contact, and log an agent in to handle and complete an outbound call. Follow the procedures in **Section 8.5** to access the Encore web interface, and log in using the appropriate credentials.

The **encore** screen is displayed with a list of call recordings. Verify that there is an entry in the right pane reflecting the last call, with proper values in the relevant fields. The screenshot below showed two entries, with the first entry containing the recording for the agent connection to the Proactive Contact welcome announcement as part of log in.



Right click on the pertinent entry and select **Play** to listen to the playback. Verify that the screen is updated and that the call recording is played back.



10. Conclusion

These Application Notes describe the configuration steps required for dvsAnalytics Encore 6.0.4 to successfully interoperate with Avaya Proactive Contact 5.1.1 with CTI and Avaya Aura® Application Enablement Services 6.3.3. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

11. Additional References

This section references the product documentation relevant to these Application Notes.

1. *Administering Avaya Aura® Communication Manager*, Document 03-300509, Issue 10, Release 6.3, June 2014, available at <http://support.avaya.com>.
2. *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 6.3, 02-300357, June 2014, available at <http://support.avaya.com>.
3. *Administering Avaya Proactive Contact*, Release 5.1, April 2013, available at <http://support.avaya.com>.
4. *Avaya Aura™ Communication Manager TSAPI Integration Guide*, Encore Version 6.0.4, July 9, 2015, available from dvsAnalytics Support.
5. *Avaya Aura™ Communication Manager TSAPI Installation Addendum*, Release 2.3.7, July 9, 2015, available from dvsAnalytics Support.
6. *Avaya Proactive Contact Dialer Integration Guide*, Encore Version 6.0.4, June 27, 2015, available from dvsAnalytics Support.
7. *Avaya Proactive Contact Dialer Installation Addendum*, Includes Version 6.0.4, System Version 2.3.7, June 27, 2015, available from dvsAnalytics Support.

©2015 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.